



GovCertUK Security Advisory

Emails containing embedded hyperlinks pointing to RAR files

GovCertUK have detected a number of emails containing embedded hyperlinks which point to RAR files. These emails should be dismissed as spam by most spam filters however GovCertUK feel it necessary to create awareness with the goal of minimizing possible compromise.

These emails typically contain a sales pitch for an item and claim that the RAR file contains further information. If the user responds by clicking the link and downloading the RAR file upon extraction they may see valid JPGs of the item and also a file with a '.exe' extension. This claims to be a video of the product however it is a malicious executable which will compromise the machine on which it is run.

GovCertUK recommends that unsolicited emails containing hyperlinks pointing to RAR files should be discarded.